

FEDERAL BUREAU OF INVESTIGATION
FOI/PA DELETED PAGE INFORMATION SHEET
FOIPA Request No.: 1402995-000
Civil Action No.: 19-cv-1495

Total Withheld Page(s) = 25

Bates Page Reference	Reason for Withholding (i.e., exemptions with coded rationale, duplicate, sealed by order of court, etc.)
FBI(19-cv-1495)-19	(b)(7)(E)-1
FBI(19-cv-1495)-32	(b)(6)/(b)(7)(C)-1, 3
FBI(19-cv-1495)-49	(b)(3)-1; (b)(6)/(b)(7)(C)-1
FBI(19-cv-1495)-50	(b)(3)-1; (b)(6)/(b)(7)(C)-3
FBI(19-cv-1495)-52	(b)(3)-1; (b)(6)/(b)(7)(C)-1, 4
FBI(19-cv-1495)-65	(b)(3)-1; (b)(6)/(b)(7)(C)-1, 5
FBI(19-cv-1495)-69	(b)(6)/(b)(7)(C)-1, 3; (b)(7)(E)-1
FBI(19-cv-1495)-70	(b)(6)/(b)(7)(C)-1, 2, 5; (b)(7)(E)-1
FBI(19-cv-1495)-72	(b)(6)/(b)(7)(C)-1; (b)(7)(E)-1
FBI(19-cv-1495)-73 thru FBI(19-cv-1495)-88	(b)(7)(E)-1

```

XXXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)     X
X   No Duplication Fee  X
X   For this Page       X
XXXXXXXXXXXXXXXXXXXXXXXXX

```

b6 -1
b7C -1

SEARCHED
SERIALIZED
INDEXED
FILED
MAR 28 2002
FBI - NEW YORK

b6 -1
b7C -1

WITH/TEXT

WITH/OUT TEXT

BY

DATE 3-7-02

MAR 28 2002

FBI - NEW YORK

801.wpd

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

[redacted]

SEARCHED [redacted] INDEXED [redacted]
SERIALIZED [redacted] FILED [redacted]
MAR 28 2002
FBI - NEW YORK

UPLOADED
WITH/TEXT
WITH/OUT TEXT
BY [redacted]
DATE 3-7-02

801.wpd

To: Counterterrorism

From: SAC, New York

Re: [REDACTED], Date 01/23/2002

b3 -2

b7E -3

System Data:

Hardware/configuration (CPU): Various

Operating System: Various

Software: Various

Security Features:

Security Software Installed: x yes (identify firewalls, router)

Logon Warning Banner: x yes no

INTRUSION INFORMATION

Access for intrusion: x Internet connection ☐ dial-up number ☐ LAN (insider)

If Internet: Internet address: TBD

Network name: TBD

Method:

The individual who caused the intrusion first performed a port scan on their system identifying the vulnerable ports. Once he identified the vulnerable ports he performed an exploit on the ports gaining access the the outer network. Once inside he was able to obtain employees userids' and social security numbers. He activated guessed the password of a former employee's userid and gained access to the internal network. Once inside he left a password behind so that he could access the system at a later date. He also left his name behind in another system as a type of fingerprint that he had been there. The hacker, Adrian Lamo, held a press conference and admitted to committing the hack.

Path of intrusion: TBD

addresses: 1. TBD

country: 1. USA

facility: 1. TBD

Subject: ADRIAN LAMO

Age: 21

Race: W

Sex: Male

Education: unknown- well known hacker

Alias(s): Motive: Bragging rights

and theft of userids and passwords

Group Affiliation:

Employer:

Known Accomplices:

Equipment used:

Hardware/configuration (CPU):

To: Counterterrorism

From: SAC, New York

Re: [REDACTED], Date 01/23/2002

b3 -2

b7E -3

Operating System: _____
Software: _____

Impact:

Compromise of classified information: ☐ yes x no

Estimated number of computers affected: 4

Estimated dollar loss to date: over \$5000

Category of Crime:

Impairment:

- x Malicious code inserted
- Denial of service
- Destruction of information/software
- x Modification of information/software

Theft of Information:

- ☐ Classified information compromised
- x Unclassified information compromised
- x Passwords obtained
- Computer processing time obtained
- Telephone services obtained
- Application software obtained
- Operating software obtained

Intrusion:

- x Unauthorized access
- ☐ Exceeding authorized access

REMARKS

Have spoken with [REDACTED] of the Southern District of New York and complaintant.

b6 -4

b7C -4

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

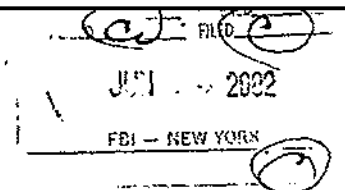
b6 -1
b7C -1

(T) [redacted] b3 -2
(F) [redacted] b7E -3

Item	Date Filed	To be returned		Dispo
		Yes	No	
1A1	6/14/02	-		CD-ROM Containing [redacted] b6 -2,-3
1A2	6/14/02	-		Orig (1) Interview [redacted] b7C -2,-3
				[redacted] b3 -2
				[redacted] b7E -3
				[redacted] b7D -1, 1M
1A3	6/14/02	-		Orig (1) [redacted] - The New York Times
1A4	6/14/02	-		(1) [redacted] - The New York Times
1A5	6/14/02	-		Original (1) [redacted]
1A6	6/14/02	-		Orig (1) [redacted] - The New York Times
1A7	6/20/02	✓		Original notes re interview (1) [redacted] The New York Time.
1A8	7/29/02	✓		(1) Disk containing logs from Lexis-Nexus regarding accounts set up by Lamo
1A9	8/19/02	✓		Hotmail.com Printout relating to email sent from [redacted] to adrian@adrian.org

DO NOT Enter Any more 1A's
see the next Volume.

[redacted] b3 -2
b7E -3



Universal Case File Number [REDACTED]

Field Office Acquiring Evidence OC

Serial # of Originating Document [REDACTED]

Date Received 4-06-2002

From [REDACTED]

(Name of Contributor)

(Address of Contributor)

(City and State)

By S4 [REDACTED]b6 -1
b7C -1To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ NoTitle: ADRIAN LAMO;
NY TIMES - VICTIMReference: _____
(Communication Enclosing Material)Description: ☐ Original notes re interview ofCD-ROM containing [REDACTED]

b7D -1

DOC LAB NOTE

DOCUMENT (S) CANNOT BE SCANNED

DESCRIPTION:

CD-Rom

Universal Case File Number [redacted]

Field Office Acquiring Evidence

NYD

Serial # of Originating Document _____

Date Received

03.14.02

From [redacted]

(Name of Contributor)

WORLDWIDE

(Address of Contributor)

(City and State)

By _____

To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title: _____

Reference: _____

(Communication Enclosing Material)

Description:

☒ Original notes re interview of

① interview [redacted]

b6 -2
b7C -2

WORLD.COM

3/14/02

[redacted] TOLD ME TO CALL

b6 -2
b7C -2

Engineers spoke w/ him (L) [redacted]

11/30/2001 - notified

- in several months, said he found vulnerability
said busy set it aside (said doing research, development
seeing what he had access to

he ~~called public re~~

investigative
↓ in CA due to
cybercrime

b6 -3
b7C -3

- he called Security Focus & [redacted] called
general desk public relations called World.com

he discussed that (L) hacked public relations
forks

- discussed internally →

lawyers - [redacted]

b6 -2
b7C -2

→ were able to verify that he had
intruded, set up call, engineers spoke
w/ him, he gave # of captured screens
of internal web-sites

- used http daemon, open proxy
 found misconf, have proxy service
 his system, port 80 was what he
 came in on, was able to view
 confidential info, got intranet website^{pages}
 was not able to tell through

- Captured files

- have all the images that he
 sent

- did not go back; do tracing,
 using one of their servers as
 his front. Was it the web site

- Said he was in a Kinko's using
 system.

- conversations were ^{not} [redacted] - Internal data network group.

b6 -2
 b7C -2

had a monetary loss.
-loss was \$

-he did not fix the system, thanked him for pointing it out, he told them how

web server \Rightarrow proxy misconfigured

fixed w/in a few minutes.

- he had unauthorized access, they would be willing to prosecute
- open proxy hunter reports back every server w/ configuration
- \$ did not want \$, looks more detrimental

Universal Case File Number [redacted]

Field Office Acquiring Evidence NYO

Serial # of Originating Document [redacted]

Date Received 2/27/2002

From [redacted]

(Name of Contributor)

(Address of Contributor)

(City and State)

By [redacted]

To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ NoGrand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title:

Reference:

(Communication Enclosing Material)

Description: ☒ Original notes re interview of① [redacted] The New York Timesb6 -2
b7C -2

→ announced he did it, track down what he said he did, left password + wrote his name in got into the outer circle, some parts got in that were open used port scan, entered circulation area (more papers, stops/starts), names of employees were there, able to run password program → former employee last 4 digits social security, guy had supervisory rights, got beta database (developing grey area)

b6 -2
b7C -2

PLEASE DO NOT REMOVE
THIS SLIP FROM EXHIBIT

b3 -2
b7E -3

Universal Case File Number [redacted]

Field Office Acquiring Evidence NYO

Serial # of Originating Document _____

Date Received 3/26/2002

From [redacted]

(Name of Contributor)

b6 -2
b7C -2The New York Times

(Address of Contributor)

(City and State)

By _____

To Be Returned ☐ Yes ☒ NoReceipt Given ☐ No ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title: _____

Reference: _____

(Communication Enclosing Material)

Description: ☐ Original notes re interview of① [redacted] - The New York Timesb6 -2
b7C -2

PLEASE DO NOT REMOVE

b6 -2
b7C -2
b3 -2
b7E -3

-

Corporate comm Group
does PR website
- digital - NY website : Boston.com

37th / 7th

- own Boston Globe

- 2/26 - called from SecurityFocus.com

b6 -2, -3
b7C -2, -3

→ gained access -

called *

once got called call different areas,
called him

did
not give name @ first, hacker
was fine w/ them contacting him.

- never spoke w/ Lamo directly
- Washington Post called were sent
screen shots by Lamo, MSNBC.

- reporter called said hacked laptop before

- [redacted] wanted comment & Confirmation

b6 -3
b7C -3

Same 415. 505. 4225 (cell)

- [redacted] called yesterday → for an update

- JeonTV heard rumor that we were going to prosecute Same.

- [redacted] asked if reporting it as a criminal act to the FBI

b6 -2
b7C -2

- Computer Security →
Hewitt Group

[redacted]

- got into a BETA database

[redacted] - put together some stuff

- ruin OPEP reputation

FD-340 (7-19-00)

b6 -1
b7C -1

Universal Case File Number [redacted]

b3 -2
b7E -3

Field Office Acquiring Evidence N40

Serial # of Originating Document [redacted]

Date Received 6/16/02

From [redacted]

b6 -2
b7C -2

(Name of Contributor)

The New York Times

(Address of Contributor)

(City and State)

By [redacted]

b6 -1
b7C -1

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title:

Reference:

(Communication Enclosing Material)

Description: ☒ Original notes re interview of

(1)

b6 -2
b7C -2



b6 -2
b7C -2
b6 -1
b7C -1

6/6/02

NEW YORK TIMES

X

- KNEW WHERE HE WAS BECAUSE HE SAID WHERE IT WAS
- ACCESS LOGS

b7E -1

had advertise web-site to redirect traffic to

Proxy redirects to

PLEASE DO NOT REMOVE

b3 -2
b7E -3

could see links through proxy server

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC

b6 -1
b7C -1

Universal Case File Number [redacted]

Field Office Acquiring Evidence NYO

Serial # of Originating Document _____

Date Received 6/6/02

From [redacted]

(Name of Contributor)

The New York Times

(Address of Contributor)

b6 -2
b7C -2

By [redacted]

b6 -1
b7C -1To Be Returned ☐ Yes ☒ NoReceipt Given ☐ ☒ NoGrand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title: _____

Reference: _____

(Communication Enclosing Material)

Description: ☒ Original notes re interview of① [redacted] The New
York Timesb6 -2
b7C -2

[redacted] (LNG), 05:48 PM 3/12/02 -0500, Re: Information on ids

b6 -2,-6
b7C -2,-6

To: [redacted] (LNG)" [redacted]
From: [redacted]
Subject: Re: Information on ids
Cc:
Bcc:
Attached:

[redacted]

b6 -6
b7C -6

Could you determine for me whether any other IDs were created on the Times account between 2/17 and 2/28? I'd like to see a list of them if you can do it.

I'll probably have you kill any that I cannot readily identify.

Thank you.

[redacted]

b6 -2
b7C -2

At 05:43 PM 3/12/02 -0500, you wrote:

[redacted]

Here is the information that you requested:

Usage started on the days they were established:

[redacted] 2002-02-19 10:00:18.953
[redacted] 2002-02-18 04:57:46.430

*dates
acct's.
set
up.*

b6 -2,-6
b7C -2,-6

Let me know if you need anything else.

[redacted]

[redacted]

[redacted]

Phone: [redacted]

Fax: 212-309-7835

[redacted]

research services

- puts up on newsmag pages
- site licenses (get)

- In March Admin looked up on Lexis Accts.
have self registration page on Intranet,
if you can get to page's have
times email acct you can register
for Lexis (does not need to be
a real times email acct)

- acct is structured in pay one sum
- saw use from one particular passport
did not know name

- went to News Admin asked if on
Staff - NO, freelancers do not
have access to email accts, NO
one who was freelancer who was
former employee

[redacted] - NEXIS representative

think maybe someone who hacked network
most use came from Kinko's in CA.
Oxnard.

- asked for any passwords

2/17 -

↑

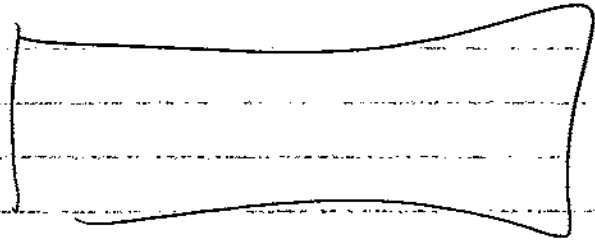
1st time saw use.

2 created then there was a

3rd will get
POLME, people could not be

identified as employees. (had her kill
the 3 passwords - date unknown.

- Activity reports



- Dow Jones Interactive contacted to
FBI (self registration PAGE) too → FBI(19-cv-1495)-24

- SAMPLE REG. PAGE
COST ANALYSIS

4 hrs of computer
time.

3

checked w/ them will provide contact
information

- time logs

- Kevin's News searches

- full access for everyone in newsroom

Are there groups set up?

yes. (part of newsroom group to
create accs.)

- anyone who has access to
network / advertising page
click if new Kevin's user

5% not
covered by
contract pay
as you go.
not created
At generic
PAGE.

- Can Cause to be saved automatic login

- have to do from inside network,

Navigator page / resource page are

intranet pages

able to ACCESS
REGISTRATION
PAGE.

FD-340 (7-19-00)

b6 -1
b7C -1

b3 -2
b7E -3

Universal Case File Number [redacted]

Field Office Acquiring Evidence

NYO

Serial # of Originating Document [redacted]

Date Received

2/26/2002

From [redacted]

(Name of Contributor)

The New York Times

(Address of Contributor)

(City and State)

By _____

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title: _____

Reference: _____

(Communication Enclosing Material)

Description: ☒ Original notes re interview of

① [redacted] The New York Times

b6 -2
b7C -2

3.26.02

- Computer Systems of Newshroom.

b6 -2
b7C -2

- added himself TechNews
retrosource DB
Contributor OPED page
housed on one server (both)

- looked @ web logs, searched for
proxy ip's found in logs.

- breach was through proxy

- searched logs proxy servers.

- sorted into X-Cell spreadsheet.

[Used logs] - times in Greenwich times
subtract 5 hours.

- looked @ DB to see entries
he put in - [need DB]

- started on the 14th

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC

b6 -1
b7C -1

- found Newshroom homepage →
~~newsource~~ news source link

- used in
could not tell if he downloaded
anything.

Reverse IP's

They knew of ip address . 203E. 204
believe they did check other
IP's address must talk to other
Tech area.

Universal Case File Number

Field Office Acquiring Evidence

NYD

Serial # of Originating Document

Date Received

7/18/02

From

Lexis - Nexus

(Name of Contributor)

(Address of Contributor)

(City and State)

b6 -1

b7C -1

By

To Be Returned

☐ Yes☒ No

Receipt Given

☐☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes☒ No

Federal Taxpayer Information (FTI)

☐ Yes☒ No

Title:

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UCb6 -1
b7C -1

Reference:

PLEASE DO NOT REMOVE

THIS CLIP FROM EXHIBIT

b3 -2
b7E -3

Description:

☐ Original notes re interview of

① Disk containing logs from Lexis-Nexus
regarding accounts set up by Lamo.

DOC LAB NOTE

DOCUMENT (S) CANNOT BE SCANNED

DESCRIPTION:

Disk

Universal Case File Number [redacted]

Field Office Acquiring Evidence NY

Serial # of Originating Document [redacted]

Date Received 9-6-2002

From [redacted]

(Name of Contributor)

(Address of Contributor)

(City and State)

By SA [redacted]b6 -1
b7C -1To Be Returned ☐ Yes ☒ NoReceipt Given ☐ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title:

Reference:

(Communication Enclosing Material)

Description: ☐ Original notes re interview ofHotmail.com printout relating
to email sent from [redacted]
to adrian@adrian.orgb6 -3
b7C -3

Sub-wpd

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

[redacted]

SEARCHED [initials] INDEXED [initials]
SERIALIZED [initials]
MAR 6 2002
FBI NEW YORK
[redacted] [initials]

b3 -2
b7E -3
b6 -1
b7C -1

b6 -1
b7C -1

UNCLASSIFIED
WITH [redacted]
WITH [redacted]
BY [initials]
DATE 3-13-02

(01/26/1998)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/06/2002

To: New York

From: New York

Squad C-37

Contact: SA [redacted]

b6 -1
b7C -1

Approved By: [redacted]

Drafted By: [redacted] slf

Case ID #: [redacted] (~~Pending~~)

b3 -2
b7E -3

Title: LAMO, ADRIAN

Synopsis: Request to open sub-files and change of title.

Details: Writer requests the following sub-files to be opened in above referenced case:

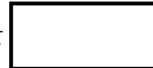
Also, please open the following Sub files:

b3 -2
b7E -3

Writer requests Title of Case be changed to :

ADRIAN LAMO
New York Times-Victim;
Computer Intrusion-Information Systems
OO:NY

♦♦



b3 -2
b7E -3
b7C -1

UPLOADED

WITH/TEXT ✓
WITH/OUT TEXT _____
BY (C) _____
DATE 3-19-02

SEARCHED (C) INDEXED (C)
MAR 11 2002
[Redacted Box]

b6 -1
b7C -1

all work @

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 03/14/2002

To: All Field Offices

Attn: NIPC SSA

From: New York

Squad C-37

Contact: SA [redacted]

b6 -1
b7C -1

Approved By: [redacted] *LM*

Drafted By: [redacted]

slf

Case ID #: [redacted]

~~(Pending)~~

b3 -2
b7E -3

Title: ADRIAN LAMO;
New York Times-Victim;
Computer Intrusion;
OO:NY

Synopsis: Canvass all FBI Offices for positive information regarding ADRIAN LAMO.

Details: In February 2002, LAMO discovered several misconfigured proxy servers acting as doorways between the public Internet and the New York Times' private intranet. LAMO utilized the proxy servers to gain access to the New York Times network. Once on the network, LAMO cracked a password for a userid with supervisor rights. Utilizing this userid he was able to broaden his access as well as perform certain functions within the network. LAMO had access to individuals names and Social Security Numbers. LAMO informed The New York Times of the security vulnerability through SECURITYFOCUS.COM.

LAMO has committed computer intrusions into several other corporations such as WORLDCOM, MICROSOFT, AOL, EXCITE@HOME and YAHOO. LAMO uses a "Proxy Hunter" to search the Internet for proxy servers that are misconfigured. Once he obtains this information, he configures his browser to appear and utilize the proxy server as his own. Once the computer intrusion occurs, LAMO searches the network to determine if there are any other vulnerabilities and in the case of The New York Times, left a backdoor so that he could enter at another time undetected.

Each time LAMO commits a computer intrusion on a high profile organization he reports the vulnerability and intrusion to the media causing a distrust of the company's clients. The above mentioned corporations have lost significant money and trust of their clients.

To: All Field Offices From: New York
Re: [REDACTED] 03/14/2002

b3 -2
b7E -3

b6 -3
b7C -3

LAMO has ties to former hacker [REDACTED] who was arrested by the FBI for computer intrusion/~~national~~-security charges.

The New York Office and the Southern District of New York are currently investigating LAMO and his computer intrusions.

Descriptive Data:

Main Subject

Name -	
Last:	LAMO
First:	ADRIAN
Middle:	
Race:	W
Sex:	M
SOC:	042-74-6804
Address -	
House #:	1230
Street Name:	Market Street, #106
City:	San Francisco
State:	CA
Postal Code:	94102

To: All Field Offices From: New York
Re: [REDACTED] 03/14/2002

b3 -2
b7E -3

LEAD (s):

Set Lead 1:

ALL RECEIVING OFFICES

It is requested to query logical sources and report only positive intelligence regarding known or potential actions of ADRIAN LAMO. Positive intelligence should be directed to SA [REDACTED]

b6 -1
b7C -1

♦♦

wpd

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC

b3 -2
b7E -1,-3
b6 -1
b7C -1

~~UPLOADED~~

WITH/TEXT ☒
WITH/OUT TEXT ☐
BY C
DATE 3-22-02

SEARCHED ☒ INDEXED ☒
MAR 14 2002
FBI — NEW YORK
☐

b6 -1
b7C -1

(01/26/1998)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [REDACTED]

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/14/2002

To: New York

From: New York

Squad C-37

Contact: SA [REDACTED]

Approved By: [REDACTED]

b6 -1
b7C -1

Drafted By: [REDACTED] slf

Case ID #: [REDACTED] (Pending)

b3 -2
b7E -3

Title: ADRIAN LAMO;
New York Times-Victim;
Computer Intrusion;
OO:NY

Synopsis: Request [REDACTED]

b7E -4

Details: In February 2002, LAMO discovered several misconfigured proxy servers acting as doorways between the public Internet and the New York Times' private intranet. LAMO utilized the proxy servers to gain access to the New York Times' network. Once on the network, LAMO cracked a password for a userid with supervisor rights. Utilizing this userid he was able to broaden his access as well as perform certain functions within the network. LAMO had access to individuals' names and Social Security Numbers. LAMO informed The New York Times of the security vulnerability through SECURITYFOCUS.COM.

LAMO has committed computer intrusions into several other corporations such as WORLDCOM, MICROSOFT, AOL, EXCITE@HOME and YAHOO. LAMO uses a "Proxy Hunter" to search the internet for proxy servers that are misconfigured. Once he obtains this information, he configures his browser to appear and utilize the proxy server as his own. Once the computer intrusion occurs, LAMO searches the network to determine if there are any other vulnerabilities and in the case of The New York Times, left a backdoor so that he could enter at another time undetected.

Each time LAMO commits a computer intrusion on a high profile organization he reports the vulnerability and intrusion to the media causing a distrust of the company's clients. The above mentioned corporations have lost significant money and trust of their clients.

To: New York From: New York
Re: [REDACTED] (~~Pending~~) 03/07/2002

b3 -2
b7E -3

LAMO has ties to former hacker [REDACTED], who was arrested by the FBI for computer intrusion/national security charges.

b6 -3,-4
b7C -3,-4

Writer contacted Assistant United States Attorney [REDACTED]-SDNY who concurred with the investigation.

To: New York From: New York
Re: [REDACTED] (Pending) 03/07/2002

b3 -2
b7E -3

LEAD(s):

Set Lead 1:

NEW YORK

AT NEW YORK

[REDACTED]

b7E -4

♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/07/2002

To: New York

Attn: ✓A/SSA
SA

From: New York

Squad C-37

Contact:

b6 -1
b7C -1

Approved By:

Drafted By:

ckk

Case ID #:

(Pending)

b3 -2
b7E -3

Title: LAMO, ADRIAN

Synopsis: Background information on subject and associates.

Enclosures: Copy of article 'He Hacks by Day, Squats by night'.

Details: On 03/06/2002, SA [redacted] requested the writer to conduct a logical search on Adrina Lamo. Mr. Lamo has a history of intruding into corporate systems: Yahoo (09/01); WorldCom (10/01) and The New York Times (03/02). According to ACS no other field office has initiated a case on this matter. Hence, SA [redacted] provided IRS [redacted] with an article found in Wired News (<http://wired.com/news/0,1294,50811,00.html>) as a starting source of information on Adrian Lamo.

b6 -1,-4
b7C -1,-4

The following names were located in the above referenced article by [redacted] writer for WiredNews:

(1)Adrian Lamo (2) [redacted] (3) [redacted] (4) [redacted]
[redacted] (5) [redacted] (6) [redacted] and (7) [redacted]

b6 -5
b7C -5
b7E -2

[redacted] provided the following details on the above names:

b7E -2

UPLOADED

WITH/TEXT ✓
WITH/OUT TEXT
BY [redacted]
DATE 3-28-02

SEARCHED	INDEXED
SERIALIZED	FILED
MAR 8 2002	

b3 -2
b7E -3

b6 -1
b7C -1

To: New York From: New York
Re: [redacted] 03/07/2002

b3 -2
b7E -3

(2)

[redacted]

b6 -5
b7C -5
b7E -2

(3)

[redacted]

(4)

[redacted]

b6 -5
b7C -5
b7E -2

(5)

[redacted]

[redacted]

b7E -2

To date, SA [redacted] has [redacted]

[redacted]

In addition, IRS [redacted] is still

[redacted]

Any further information will be

submitted to case file.

b6 -1,-4
b7C -1,-4
b7E -1,-4

♦♦

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 04/09/2002

To: New York

Attn: SA [redacted]

Squad C-37

From: Chicago

Squad IPC

Contact: SA [redacted]

b6 -1
b7C -1

Approved By: [redacted] RY

Drafted By: [redacted] jt

Case ID #: [redacted]

(Pending)

b3 -2
b7E -3

Title: ADRIAN LAMO;
NEW YORK TIMES-VICTIM;
COMPUTER INTRUSION;
OO:NY

(W)

Synopsis: Lead Covered for Chicago Division.

Reference: [redacted]

Details: As per telephone conversataion between writer and SA [redacted] on 04/04/2002, members of Chicago's Computer Intrusion Squad (IPC) were canvassed regarding the referenced EC with negative results. ACS was also canvassed for any related Chicago Division cases with negative results.

b6 -1
b7C -1

Chicago considers this lead covered.

♦♦

[redacted]

b3 -2
b7E -3

SEARCHED
SERIALIZED FILED

MAY 07 2002

[redacted]

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 04/16/2002

To: New York

Attn: SA [redacted]
Squad C-37

From: Washington Field

NS-18 / Northern Virginia Resident Agency

Contact: [redacted]

b6 -1
b7C -1

Approved By: [redacted] *scj/mz*

Drafted By: [redacted] *:sjp*

Case ID #: [redacted] (Pending)

Title: ADRIAN LAMO;
New York Times-Victim;
Computer Intrusion;
OO:NY

b3 -2
b7E -3

Synopsis: Lead covered at WFO.

Reference [redacted]

Administrative: Reference March 22, 2002 email sent to SSA
[redacted] from SSA [redacted]

b6 -1
b7C -1

Details: Referenced communication requested WFO/NIPC query
logical sources and report only positive intelligence
regarding known or potential actions of ADRIAN LAMO.

SSA [redacted] sent SSA [redacted] via
email, information advising that Ameritech/SBC was a victim of
Adrian Lamo. SSA [redacted] additionally stated that he believes
that Ameritech/SBC spoke with FBI Dallas concerning this.

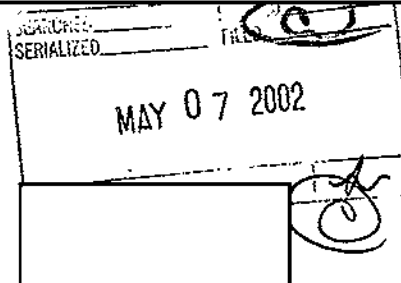
b6 -1
b7C -1

All other logical sources were queried, however, no
positive information was provided.

Based on the above investigation, and unless advised
by New York Division, WFO considers this lead covered. No
further investigation regarding this lead will be performed. Any
questions regarding this matter should be directed to SA [redacted]
at [redacted]

b6 -1
b7C -1
b3 -2
b7E -3

sp021071.ec



FBI(19-cv-1495)-46

To: New York From: Washington Field
Re: 04/16/2002

b3 -2
b7E -3

LEAD(s) :

Set Lead 1:

NEW YORK

AT NEW YORK, NY

Read and clear.

♦♦

sp021071.ec

2

FBI(19-cv-1495)-47

Requested from AUSA [redacted]
[redacted] on 4/2/02 via email.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

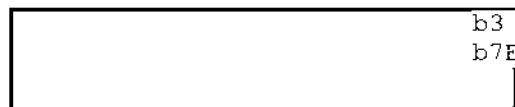
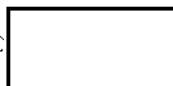
b6 -1
b7C -1

[redacted] b3 -2
b7E -3

SEARCHED	INDEXED
SERIALIZED	FILED
APR 03 2002	
[redacted]	

b6 -1,-4
b7C -1,-4

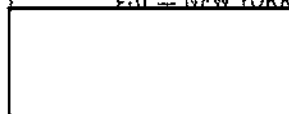
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC



b3 -2
b7E -3

SEARCHED INDEXED
SERIALIZED FILED
APR 03 2002
FBI - NEW YORK

b6 -1
b7C -1



[Handwritten signature]

b6 -1
b7C -1

(01/26/1998)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/08/2002

To: New York

From: New York

C-37

Contact: [redacted]

Approved By: [redacted]

b6 -1
b7C -1

Drafted By: [redacted] tk

Case ID #: [redacted] (Pending)
(Pending)✓

b3 -2
b7E -3

Title: [redacted]

Synopsis: Use of [redacted] to provide [redacted]
Internet access.

b6 -1
b7C -1
b7E -1,-4

Details: On 03/08/02 writer provided SA [redacted] with
[redacted] to the Internet through the
[redacted] SA [redacted] utilized the [redacted]
[redacted]

SA [redacted] was able to begin an investigation on subject
ADRIAN LAMO. LAMO has comitted computer intrusions into several
corporations such as WORLDCOM, MICROSOFT, AOL and EXCITE@HOME.
LAMO posts his "accomplishments" to the media and on
SECURITYFOCUS.COM web site. To help SA [redacted] ongoing
investigation, writer will continue to provide use of [redacted]
[redacted]

b6 -1
b7C -1
b7E -1

♦♦

b3 -2
b7E -3

[redacted]	
SEARCHED	INDEXED
SERIALIZED	FILED
APR 2002	
[redacted]	

b6 -1
b7C -1

How LAMO, WPD
UNLOADED
WITH/TITLE
WITH/TITLE
BY [redacted]
DATE 4-23-02

FBI(19-cv-1495)-53

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 05/20/02 Time: 09:18

Case ID:

b3 -2
b7E -3

Description of Document:

Type : FD302
Date : 03/19/02
To : WASHINGTON FIELD
From : NEW YORK
Topic: ON 3-19-02, A COMMUNICATION VIA FAX WAS RECEIVED IN RESPONSE

Reason for Permanent Charge-Out:

WRONG FILE NUMBER

Employee:

b6 -1
b7C -1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

[redacted]		b3 -2 b7E -3
SERIALIZED	FILED	b6 -1 b7C -1
MAY 07 2002		
[redacted]		b6 -1 b7C -1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [REDACTED]

b6 -1
b7C -1

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/19/2002

Individual, who has not agreed to testify, provided the following information:

b6 -3
b7C -3
b7D -1

[Handwritten signature]

Investigation on 04/06/2002 at [REDACTED]File # [REDACTED] Date dictated 04/19/2002

by SA [REDACTED] mth

b3 -2
b6 -1
b7C -1
b7D -2
b7E -3

✓ 802109H1, MTH

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FBI(19-cv-1495)-56

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 04/19/2002

To: New York

Attn: Squad C-37

SA [redacted]

b6 -1
b7C -1

From: Oklahoma City

Squad 8

Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

dwz

Case ID #: [redacted]

(Pending) [redacted]

b3 -2
b7E -3

Title: ADRIAN LAMO;
New York Times - Victim;
Computer Intrusion;
OO:NY

Synopsis: To cover lead.

Reference: [redacted]

Enclosure(s): 1) One original and one copy of a source 302
referencing Lamo;

2) One IA envelope containing [redacted]

b7D -1

Details: In response to NY Division lead, OC Division queried
all sources for information on Lamo. The results of the inquiry
are located in the enclosures.

OC Division considers this lead completed.

b3 -2
b7E -3

LEAD/ASSIGN/COVERED
DATE 5/30/02
ASSIGN TO
SUPV. [redacted]

No lead for this
serial @

[redacted]

SEARCHED	INDEXED
SERIALIZED	FILED
MAY 07 3 00 2002	
FBI - NEW YORK	

[redacted]

SEARCHED	INDEXED
SERIALIZED	FILED
MAY 30 2002	
FBI - NEW YORK	

b6 -1
b7C -1

80210924 du3

To: New York From: Oklahoma City
Re: 04/19/2002

b3 -2
b7E -3

LEAD(s):

Set Lead 1: (Adm)

NEW YORK

AT NEW YORK, NY

Read and clear.

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC

UPLOADED

WITH/TEXT ☒
WITH/OUT TEXT ☐
BY C
DATE 5-13-02

SEARCHED ☒ INDEXED ☒
SERIALIZED ☒ FILED ☒

MAY 09 2002

FBI - WASH DC

b3 -2
b7E -3
b7C -1

b6 -1,-2
b7C -1,-2

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/09/2002

[redacted]
WORLD COM telephone number (972) 729-7108 was telephonically contacted by interviewing agent. After being advised as to the identity of the interviewing agent and the purpose of the interview, [redacted] provided the following information:

b6 -2
b7C -2

[redacted] is aware of an individual by the name of ADRIAN LAMO. LAMO hacked into the computer network of WORLD COM in November 2001.

WORLD COM's Public Relations Department was contacted by [redacted] Security Focus, and informed that LAMO had hacked into their network. [redacted] and his engineers were able to confirm that there was an intrusion into their network. The engineers, [redacted] and [redacted] Internal Data Network Group, along with a member of WORLD COM's Legal Department [redacted] arranged a telephone call between themselves and LAMO. LAMO provided WORLD COM with internal screen captures that he had obtained when he had hacked into their network. The screen captures contained information pertaining to their internal web-sites. [redacted] stated that LAMO gained unauthorized access to their networks to obtain the screen captures and any other information.

b6 -2,-3
b7C -2,-3

LAMO told WORLD COM employee's that he gained access to their internal network through a misconfigured proxy server. LAMO exploited Port 80 on the proxy server and once he gained access he was able to view confidential information on WORLD COM's internal network. LAMO admitted to the WORLD COM employees that he accessed their network from KINKOS. LAMO informed WORLD COM about the intrusions months after he had first intruded. The engineers immediately reconfigured the proxy server to prevent against future exploits of this kind.

[redacted] said that WORLD COM suffered a significant financial loss due to the unauthorized intrusion by LAMO. [redacted] believes that LAMO was looking for publicity not monetary rewards for his hacking. The publicity that WORLD COM received because of the intrusion was detrimental to WORLD COM's business.

b6 -2
b7C -2Investigation on 03/14/02 at New York, NY (telephonically)

File #

Date dictated 03/17/2002

by SA [redacted]

b6 -1
b7C -1
b3 -2
b7E -3

b6 -2,-3
b7C -2,-3
b3 -2
b7E -3

Continuation of FD-302 of [REDACTED], On 03/14/02, Page 2

[REDACTED] stated that a WORLDCOM investigator was familiar with [REDACTED]. In the past, the investigator had arrested [REDACTED] in California for hacking into unauthorized systems.

Insert:wpd

[Redacted]

b3 -2
b7E -3

UPLOADED

WITH/TEXT ✓
WITH/OUT TEXT _____
BY C
DATE 5-28-02

SEARCHED	INDEXED
SERIALIZED	FILED
MAY 25 2002	
[Redacted]	

b6 -1
b7C -1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [Redacted]

b6 -1
b7C -1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC

b6 -1
b7C -1
b3 -2
b7E -3

[REDACTED]
05/07/2002
CAH:cah

Attached is a letter received in response to a subpoena sent
to [REDACTED]
[REDACTED]

b3 -1



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC

b3 -21
b7E -31

[REDACTED]
05/07/2002
CAH:cah

Attached is a letter received in response to a subpoena sent
to [REDACTED]
[REDACTED]

b3 -1

FBI(19-cv-1495)-64

[REDACTED]
b3 -2
b7E -3

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC

UPLOADED

WITH/TEXT
WITH/OUT
BY
DATE 6-12-02

b3 -2
b7E -3
b7C -1

SEARCHED
SERIALIZED
JUN 1 0 2002
FBI - NEW YORK

b6 -1,-2
b7C -1,-2

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/27/2002

[REDACTED] Publishing Systems, THE NEW YORK TIMES, 229 West 43rd Street, New York, NY 10036, telephone number [REDACTED] was interviewed at her place of employment. Also present during the interview was [REDACTED] of THE NEW YORK TIMES. After being advised as to the identities of the interviewing agents and the purpose of the interview, [REDACTED] provided the following information:

b6 -2
b7C -2

[REDACTED] is aware of the computer intrusion into THE NEW YORK TIMES intranet by ADRIAN LAMO. [REDACTED] believes that LAMO gained unauthorized access to their intranet on or around February 14, 2002. [REDACTED] along with members of her staff reviewed the logs of their web servers and proxy servers and from this they were able to determine that LAMO had gained unauthorized entry to their intranet through one (1) of their proxy servers. The IP addresses of the proxy servers that were reviewed were [REDACTED] and [REDACTED]

b6 -2
b7C -2
b7E -1

LAMO was able to access the newsroom's intranet homepage. Through this homepage he was able to add himself and view the data [REDACTED]

b6 -2
b7C -2
b7E -1

[REDACTED] reviewed the database and was able to view the unauthorized entries made by LAMO. At this time, [REDACTED] is unable to determine if LAMO downloaded any information from their intranet.

[REDACTED] provided the interviewing agents with a copy of emails and analysis reports prepared regarding the computer intrusion of LAMO. [REDACTED] stated that the logs and database will be secured by THE NEW YORK TIMES.

b6 -2
b7C -2Investigation on 03/26/2002 at New York, NYFile # [REDACTED] Date dictated 03/27/2002by SA [REDACTED]
SA [REDACTED]b6 -1
b7C -1
b3 -2
b7E -3

[redacted] 05:55 PM 2/28/02 -0500, web logs

X-Sender: [redacted]
X-Mailer: QUALCOMM Windows Eudora Version 4.3.2
Date: Thu, 28 Feb 2002 17:55:35 -0500
To: [redacted]
From: [redacted]
Subject: web logs

[redacted] and found indications that our
hacker friend was in the system as early as February 14 and as recently as February 25. He did
this by [redacted]

b6 -2
b7C -2
b7E -1

[redacted] Here's the summary of hits on the technews server.
Times were originally logged in Greenwich Mean Time; I've converted them to Eastern by
subtracting five hours.

Thursday, Feb. 14 58 hits between 1:36 a.m. and 2:24 a.m.
Wednesday, Feb. 20 326 hits between 7:44 p.m. and 10:41 p.m.
Thursday, Feb. 21 95 hits between 10:06 a.m. and 10:55 a.m.
Monday, Feb. 25 98 hits between 3:00 p.m. and 3:45 p.m.
Tuesday, Feb. 26 30 hits between 8:00 a.m. and 8:15 a.m.

A "hit" is either a "get" or a "post". A "get" is a request for information, or a read. A "post" is a
"write". On [redacted] logs, there are 441 gets and 166 posts.

b6 -2
b7C -2

[redacted]
The New York Times
Seventh Floor, 229 West 43rd Street
New York, NY 10036-3959
Phone: [redacted] Pager: [redacted] Fax: 212-556-1636

Printed for [redacted]

[redacted] 10:59 AM 3/26/02 -0500, FW: Change in Stafflist

From: [redacted]
To: [redacted]
Subject: FW: Change in Stafflist
Date: Tue, 26 Mar 2002 10:59:33 -0500
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2911.0)
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
Importance: Normal

← newroom admin
ob DB, everytime new
user added he gets
an email → on
vacation @ the
time.

-----Original Message-----

From: [redacted]
Sent: Wednesday, February 20, 2002 8:10 PM
To: [redacted]
Subject: Change in Stafflist

[redacted] Add [redacted]

get this email file

Printed for [redacted]

1

b6 -2
b7C -2

FBI(19-cv-1495)-71

wpd

UPLOADED

WITH/TEXT ☒
WITH/OUT TEXT ☐
BY ca
DATE 6-12-02

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC



SEARCHED	INDEXED
SERIALIZED	FILED
JUN 10 2002	
FBI - NEW YORK	



b3 -2
b7E -3

b6 -1,-2
b7C -1,-2

b6 -1
b7C -1

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/27/2002

[redacted] Public Relations, THE
NEW YORK TIMES, 229 West 43rd Street, New York, NY 10036, telephone
number, [redacted] was interviewed at her place of employment.
Also present during the interview was [redacted]
[redacted] THE NEW YORK TIMES. After being advised as to
the identities of the interviewing agents and the purpose of the
interview, [redacted] provided the following information:

b6 -2
b7C -2

On February 26, 2002, [redacted] was connected by [redacted]
[redacted] of SECURITYFOCUS.com. [redacted] informed THE NEW YORK TIMES
that an individual had gained access to their intranet and asked
for a comment from them. [redacted] provided his telephone number
[redacted] and email address [redacted]
[redacted] began calling the areas necessary to confirm the intrusion.

b6 -2,-3
b7C -2,-3

[redacted] was able to confirm that an intrusion had occurred
so she contacted [redacted]. When she contacted [redacted] he told her
that the hacker, ADRIAN LAMO had gained access into their intranet
and that LAMO would not have a problem if THE NEW YORK TIMES
contacted him directly. [redacted] was provided LAMO's cell phone
number (415) 505-4225. [redacted] never spoke with LAMO directly.

b6 -2,-3
b7C -2,-3

[redacted] received a telephone call from the WASHINGTON POST
and MSNBC.com and was informed that LAMO had provided them with
screen shots of their intranet and she was asked to comment. One
of the reporters who called her told her that LAMO informed them
that he had been in their intranet for 10 days prior to informing
them of the intrusion.

[redacted] commented that [redacted] called her yesterday "for an
update". [redacted] told her that he heard a rumor from TECHTV that
THE NEW YORK TIMES was going to prosecute LAMO for his unauthorized
intrusion. [redacted] wanted to know if [redacted] had reported it as a
criminal act to the Federal Bureau of Investigation.

b6 -2,-3
b7C -2,-3

[redacted] commented that LAMO ruined the reputation of their
OPED page.

Investigation on 03/26/2002 at New York, NYFile: [redacted] Date dictated 03/27/2002
by SA [redacted]
SA [redacted]b6 -1
b7C -1
b3 -2
b7E -3

b3 -2
b7E -3

Continuation of FD-302 of

, On 03/26/2002 , Page 2

b6 -2
b7C -2

 provided the interviewing agents with various paperwork regarding her discussions and investigation into the unauthorized intrusion by LAMO.

[redacted]
02/26/2002 01:11 PM

b6 -1, -2, -3
b7C -1, -2, -3

To:
cc:

Subject: Reporter call re: alleged security breach w/NYT Co. intranet

I received a call from [redacted] a reporter with Security Focus, an online publication.
(www.securityfocus.com)

[redacted] said he was contacted by a hacker of "known reliability" who said he was able to gain access to The New York Times Company's intranet (and extranet, it seems).

According to the reporter, this hacker said he was able to download the social security numbers of all Times employees, as well as personal files/info on 3,000 op-ed contributors. He also accessed credit card information for home delivery subscribers.

He said he was able to get thru via an open proxy server.

Please give me a call to let me know

- 1) if this is possible
- 2) if we can track access records to see if in fact our files were accessed by this person and
- 3) how we'd like to respond.

The reporter's on deadline for today and has asked us to comment. Supposedly this is a "friendly" hacker who in the past has alerted companies to these types of security issues and helped resolve them (not as a paid consultant but to be "helpful" according to the reporter).

thanks!

[redacted]

b6 -2
b7C -2

[redacted]

[redacted] PR

The New York Times Company

[redacted]

[redacted]
02/26/2002 02:01 PM

b6 -1, -2
b7C -1, -2

To:
cc:

Subject: Re: IP addresses for alleged security breach -- NYT intranet

[redacted] now has this information and is examining her proxy server for more information.

b6 -2
b7C -2

[redacted]
02/26/02 01:29 PM

To:
cc:

Subject: IP addresses for alleged security breach -- NYT intranet

I called back to clarify where this information was accessed so we could nail this down. Reporter also gave me the IP addresses for the proxy servers that were accessed.

-- I think it's limited to the NYT newspaper -- the social security numbers were for newspaper employees and op-ed columnists.

--I'm not sure who serves the home delivery Web site, but the hacker gave the reporter a log that had a chronological file of when print subscribers had stopped & started delivery, or complained etc.

here are the IP addresses:

[redacted]

b7E -1

I'll call to followup. thanks.

b6 -2
b7C -2

[redacted]
02/26/2002 01:11 PM

To:
cc:

[redacted]
02/26/2002 03:15 PM

b6 -1, -2, -3
b7C -1, -2, -3

To:
cc:

Subject:

I called back the reporter, [redacted] to find out his deadline. He is filing by 4 PM EST today, so we'll need to draft a holding statement by then.

[redacted] also said the hacker was fine with us to contacting him; described him as an unusual, "friendly hacker" who wants to help. I'm not sure how you've handled this in the past but here's his info:

Adrian Lamo 415-505-4225

I did a Google search on Lamo and turned up recent, similar articles by the same publication & reporter of today's query, FYI:

Yahoo! News hacked
Hacker tinkers with news articles undetected.
By Kevin Poulsen
<http://online.securityfocus.com/news/254>
Sep 18 2001 4:25PM PT

In a development that exposes grave risks of news manipulation in a time of crisis, a hacker demonstrated Tuesday that he could rewrite the text of Yahoo! News articles at will, apparently using nothing more than a web browser and an easily-obtained Internet address.

Yahoo! News, which learned of the hack from SecurityFocus, says it has closed the security hole that allowed

20-year-old hacker Adrian Lamo to access the portal's web-based production tools Tuesday morning, and modify an

August 23rd news story about Dmitry Sklyarov, a Russian computer programmer facing federal criminal charges under

the controversial Digital Millennium Copyright Act (DMCA).

Lamo's Adventures in WorldCom

The helpful hacker strikes again, this time finding a route into the communications company's private Web,

then telling its security staff all about it. Who is Adrian Lamo, why does he do this, and would his life be the

same if Kinkos kicked him out?

By Kevin Poulsen

Dec 5 2001 10:46AM PT

<http://online.securityfocus.com/news/296>

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC

[REDACTED]
02/26/2002 04:19 PM

b6 -1, -2
b7C -1, -2

To:

cc:

Subject: response to first press inquiry

am drafting the response to the second query; will circulate shortly.

----- Forwarded by [REDACTED] on 02/26/2002 04:13 PM -----

[REDACTED]
02/26/2002 04:01 PM

b6 -2, -3
b7C -2, -3

To:

cc:

Subject: NYT issue

[REDACTED]

b6 -2, -3
b7C -2, -3

I realize you're on deadline for 4 PM EST so here's a statement:

"The New York Times Company takes the security of its network very seriously and we are actively investigating a potential security breach. Based on the results of this investigation we will take appropriate steps to ensure the security of our network."

[REDACTED]

PR

The New York Times Company

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-18-2010 BY 60324 UC [redacted]

[redacted]
02/26/2002 04:16 PM

b6 -1, -2
b7C -1, -2

To: [redacted]
cc:

Subject: second press query: NYT intranet exposure

[redacted] let's talk more about pulling the site(s) down. My concern is that if [redacted]
[redacted]
[redacted]

b6 -2
b7C -2
b7E -1

This reporter is filing tonight too, and word gets around quickly in the hacker community. Don't want more folks hitting the sites.

If it's not secure, and personal info is out there, we may want to err on the side of caution until we're sure.

----- Forwarded by [redacted] on 02/26/2002 04:09 PM -----
[redacted] on 02/26/2002 03:57:28 PM

b6 -2
b7C -2

To: [redacted]
cc:

Subject: NYT intranet exposure
:

[redacted]

b6 -2
b7C -2

A source of mine tells me that the NYT Corporate Intranet was exposed via a rogue proxy on the company's netblock. He has sent me detailed screen shots and information.

I'm writing to solicit any general comments the company is prepared to make on this development. I have also included some specific questions below, if you'd care to address them.

Has the NYT disabled access to the sites in question, and had anyone there previously expressed concern that such an exposure might come to pass?

How long has remote access been available through this network? Did the Times take any steps in particular to prevent the sort of high-profile defacement left in 1998 by the group "Hackers for Girlies"?

Thanks in advance for your help. This is for a story I'm filing this afternoon. I'll call you as well.

Sincerely,

[redacted]
02/26/2002 07:32 PM

b6 -1, -2
b7C -1, -2

To:
cc:

Subject: thoughts about calling the hacker tomorrow? WorldCom did...

here's the excerpt from the article I sent earlier. WorldCom worked actively with "the kid" to fix the wholes...he also contact them through SecurityFocus.com.

I think a techie to techie call would be fine, he seems pretty helpful from this article.

And working with him would be a way to minimize the situation like WorldCom did below. let me know what you want to do...

<http://online.securityfocus.com/news/296>
Lamo's Adventures in WorldCom

The Helpful Hacker

"Vint Cerf recently did a public service announcement in which, generally speaking, the message was it would be really

great if the hacker community went back to its roots," says WorldCom spokesperson Jennifer Baker. "I guess that from

a general industry standpoint, Adrian seems to be doing just that... At that end of the day, what he did wasn't

destructive or harmful."

Over a month after the Kinkos visit, Lamo has come clean with WorldCom, and the company is grateful. The hacker

contacted the communications leviathan through SecurityFocus on Friday. Saturday morning, just as he crashed after

an all-night hacking session on "an unrelated project," his cell phone rang. There were three WorldCom managers on

the line, wondering of it was true that Lamo had cracked their global corporate intranet, and what they needed to do to fix it.

"I made it clear very quickly that all I was interested in doing was make it as positive an experience as possible for

everyone," says Lamo. True to his word, the hacker would spend the rest of the weekend on conference calls and in

email, bleary briefing the company on his months of illicit exploration. On Tuesday, the WorldCom turned to Lamo to

give them a final bill of health. After a scan of their address space, he pronounced that WorldCom had successfully closed the proxy hole.

"What we discovered when we investigated Adrian's issues, was that there was a router with an inappropriate filter on it,"

says Baker. "In the end it was a human error, and we're really happy that he brought it to our attention... We really

appreciate his efforts to work with us"

That instant willingness to cooperate, even to sign a non-disclosure agreement, with no strings attached is part of what's

kept Lamo out of legal trouble, for what are indisputably violations of federal computer crime law. In May, when the

hacker used an open proxy to crack ailing Excite@Home's internal Web, adding himself to the corporate directory and

finding a route to millions of subscribers' records, he walked into the company's Redwood City, Calif. headquarters to

brief network administrators in person, and he didn't leave before helping them plug the hole.

02/26/2002 07:37 PM

To:
cc:

Subject: some hints to the WorldCom hacking that might apply to us
from that same article. <http://online.securityfocus.com/news/296>
did he do the same on NYT Co's intranet?

The Problem with Proxies

As he has with other networks, Lamo found the keys to WorldCom's kingdom in open Internet proxy servers. In normal operation, a proxy server is a dedicated machine that sits between a local network and the outside world, passing internal surfers' Web requests out to the Internet, often caching the results to speed up subsequent visits to the same URL.

But it's easy and common for administrators to inadvertently misconfigure proxy servers, allowing anyone on the Internet to channel through them. Sometimes companies and organizations even unknowingly run proxies. Hackers and privacy-conscious netizens catalog these open proxies, using them to anonymize their surfing. **Lamo has perfected a different use: jumping through them to pose as a node on a company's internal network.**

Using a common hacker tool called "Proxy Hunter," Lamo scanned WorldCom's corporate Internet address space, and quickly found five open proxies -- one of them hiding in plain site at wireless.wcom.com. From there, he needed only to configure his browser to use one of the proxies, and he could surf WorldCom's private network as an employee.

Once inside, he found other layers of security protecting various intranet sites from employees who might exceed their

authorized access. But after a couple of months of sporadic exploring, Lamo has made substantial inroads. He can use

WorldCom human resources system to list names and matching social security numbers for any or all of the company's

86,000 employees. With this information, all he needs is a birth date (he swears by anybirthday.com) and he can reset

an employee's password and access his or her payroll records, including information like their salary, emergency

contacts, and direct deposit instructions, complete with bank account numbers. He could even modify the employee's

direct deposit bank account, and divert a paycheck to his own account, if he wanted to. "A lot of people would be willing

to blow town for a couple hundred thousand dollars," says Lamo.

AOL's

He has some access to customer records, too, primarily subscribers to WorldCom's data services. He can browse notes and circuit diagrams for

new T1 cross border link between its Virginia offices and AOL Mexico, and a detailed engineering order for a connection between the